PCT/FR2004/003252

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 18 NOV. 2004

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS
CONFORMÉMENT À LA
RÈGLE 17.1.a) OU b)

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint-Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr

1er dépôt

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11354*02

REQUÊTE EN DÉLIVRANCE
page 1/2

BR1

Cet imprimé est à remplir lisiblement à l'encre noire

DB 540 W / 010801

Réservé à l'INPI

REMISE DES PIÈCES
DATE 17 DEC. 2003
LIEU 75 INPI PARIS 34 SP
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0314833
DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 17 DEC. 2003

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

CABINET BEAU DE LOMENIE
158, rue de l'Université
75340 PARIS CEDEX 07

Vos références pour ce dossier *(facultatif)* 1H518040/22.SY

Confirmation d'un dépôt par télécopie ☐ N° attribué par l'INPI à la télécopie

2 NATURE DE LA DEMANDE	Cochez l'une des 4 cases suivantes
Demande de brevet	☒
Demande de certificat d'utilité	☐
Demande divisionnaire	☐
Demande de brevet initiale	N° Date
ou demande de certificat d'utilité initiale	N° Date
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N° Date

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Procédé de gestion d'un ensemble d'alertes issues de sondes de détection d'intrusions d'un système de sécurité d'informations.

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE

Pays ou organisation
Date N°
Pays ou organisation
Date N°
Pays ou organisation
Date N°

☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**

5 DEMANDEUR (Cochez l'une des 2 cases) ☒ **Personne morale** ☐ **Personne physique**

Nom ou dénomination sociale		FRANCE TELECOM
Prénoms		
Forme juridique		Société anonyme
N° SIREN		
Code APE-NAF		
Domicile ou siège	Rue	6 Place d'Alleray
	Code postal et ville	7 5 0 1 5 PARIS
	Pays	FRANCE
Nationalité		Française
N° de téléphone *(facultatif)*		N° de télécopie *(facultatif)*
Adresse électronique *(facultatif)*		

☐ **S'il y a plus d'un demandeur, cochez la case et utilisez l'imprimé «Suite»**

Remplir impérativement la 2ème page

1er dépôt

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE
page 2/2

BR2

Réservé à l'INPI

REMISE DES PIÈCES
DATE 17 DEC. 2003
LIEU 75 INPI PARIS 34 SP
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0314833

DB 540 W / 010801

Vos références pour ce dossier : *(facultatif)*		1H518040/22.SY
6 MANDATAIRE *(s'il y a lieu)*		
Nom		
Prénom		
Cabinet ou Société		CABINET BEAU DE LOMENIE
N °de pouvoir permanent et/ou de lien contractuel		
Adresse	Rue	158, rue de l'Université
	Code postal et ville	7 5 1 3 1 4 0 PARIS CEDEX 07
	Pays	FRANCE
N° de téléphone *(facultatif)*		01 44 18 89 00
N° de télécopie *(facultatif)*		01 44 18 04 23
Adresse électronique *(facultatif)*		
7 INVENTEUR (S)		**Les inventeurs sont nécessairement des personnes physiques**
Les demandeurs et les inventeurs sont les mêmes personnes		☐ Oui ☒ Non : **Dans ce cas remplir le formulaire de Désignation d'inventeur(s)**
8 RAPPORT DE RECHERCHE		**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé		☒ ☐
Paiement échelonné de la redevance *(en deux versements)*		**Uniquement pour les personnes physiques effectuant elles-mêmes leur propre dépôt** ☐ Oui ☐ Non
9 RÉDUCTION DU TAUX DES REDEVANCES		**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Obtenue antérieurement à ce dépôt pour cette invention *(joindre une copie de la décision d'admission à l'assistance gratuite ou indiquer sa référence)* : **AG**
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		

10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire)	Jean-Jacques JOLY CPI N° 92-1123
VISA DE LA PRÉFECTURE OU DE L'INPI	L. MARIELLO

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

Arrière-plan de l'invention

L'invention concerne un procédé de gestion d'un ensemble d'alertes issues de sondes de détection d'intrusions.

La sécurité des systèmes d'information passe par le déploiement de systèmes de détection d'intrusions « IDS » comportant des sondes de détection d'intrusions qui émettent des alertes vers des systèmes de gestion d'alertes.

En effet, les sondes de détection d'intrusions sont des composants actifs du système de détection d'intrusions qui analysent une ou plusieurs sources de données à la recherche d'événements caractéristiques d'une activité intrusive et émettent des alertes vers les systèmes de gestion d'alertes. Un système de gestion des alertes centralise les alertes provenant des sondes et effectue éventuellement une analyse de l'ensemble de ces alertes.

Les sondes de détection d'intrusions génèrent un très grand nombre d'alertes qui peut comprendre plusieurs milliers par jour en fonction des configurations et de l'environnement.

L'excès d'alertes peut résulter d'une combinaison de plusieurs phénomènes. Tout d'abord, de fausses alertes représentent jusqu'à 90% du nombre total d'alertes. Ensuite, les alertes sont souvent trop granulaires, c'est-à-dire que leur contenu sémantique est très pauvre. Enfin les alertes sont souvent redondantes et récurrentes.

Ainsi, l'excès d'alertes rend leur compréhension et leur manipulation difficile par un opérateur de sécurité humain.

Le traitement amont des alertes au niveau du système de gestion est donc nécessaire pour faciliter le travail d'analyse de l'opérateur de sécurité.

Les systèmes de gestion d'alertes actuels consistent à stocker les alertes dans un système de gestion de bases de données relationnelles (SGBDR). L'opérateur de sécurité peut ainsi interroger ce système de gestion SGBDR en lui soumettant une requête portant sur les propriétés des alertes. Le système de gestion SGBDR fournit en retour à l'opérateur, l'ensemble des alertes dont la description satisfait la requête.

L'inconvénient de ces systèmes est le fait que les alertes fournies à l'opérateur peuvent être nombreuses et granulaires, ce qui rend leur analyse fastidieuse.

Objet et résumé de l'invention

L'invention a pour but de remédier à ces inconvénients, et de fournir une méthode simple de gestion d'un ensemble d'alertes issues de sondes de détection d'intrusions pour permettre une consultation flexible, aisée et rapide de cet ensemble d'alertes.

Ces buts sont atteints grâce à un procédé de gestion d'un ensemble d'alertes issues de sondes de détection d'intrusions d'un système de sécurité d'informations comportant un système de gestion d'alertes, chaque alerte étant définie par un identifiant d'alerte et un contenu d'alerte, caractérisé en ce qu'il comporte les étapes suivantes :

-associer à chacune des alertes issues des sondes de détection d'intrusions, une description comportant une conjonction d'une pluralité d'attributs valués appartenant à une pluralité de domaines d'attributs ;

-organiser les attributs valués appartenant à chaque domaine d'attribut en une structure taxinomique définissant des relations de généralisation entre lesdits attributs valués, la pluralité des domaines d'attributs formant ainsi une pluralité de structures taxinomiques ;

-compléter la description de chacune desdites alertes par des ensembles de valeurs induites par les structures taxinomiques à partir des attributs valués desdites alertes pour former des alertes complètes ;

-stocker lesdites alertes complètes dans un système de fichiers logique pour en permettre la consultation.

Ainsi, le stockage des alertes complètes dans un système de fichiers logique permet à un opérateur de sécurité de consulter le système de gestion d'alertes d'une manière efficace, rapide, et flexible afin d'obtenir une vision précise de l'ensemble des alertes issues des sondes de détection d'intrusions.

La consultation des alertes complètes peut être réalisée par une succession d'interrogations et/ou de navigations dans lesdites alertes complètes de sorte qu'en réponse à une requête, le système de gestion d'alertes fournit des attributs valués pertinents permettant de distinguer un sous-ensemble d'alertes complètes parmi un ensemble d'alertes complètes satisfaisant la requête afin de permettre le raffinement de ladite requête.

De préférence, les attributs valués pertinents sont en priorité les plus généraux en regard de la pluralité des structures taxinomiques.

Avantageusement, en réponse à la requête, le système de gestion d'alertes fournit en outre des identifiants d'alertes satisfaisant la requête et dont la description ne peut pas être raffinée par rapport à ladite requête.

L'identifiant d'alerte est un couple formé d'un identifiant de la sonde de détection d'intrusions qui produit l'alerte et d'un numéro de série d'alerte affecté par ladite sonde.

Le contenu de chaque alerte comporte un message textuel fourni par la sonde de détection d'intrusions correspondante.

Chaque attribut valué comporte un identifiant d'attribut et une valeur d'attribut.

Selon un aspect de l'invention, chaque identifiant d'attribut est associé à un domaine d'attributs parmi les domaines suivants : domaine de l'attaque, domaine de l'identité de l'attaquant, domaine de l'identité de la victime et domaine de la date de l'attaque.

Avantageusement, la description d'une alerte donnée est complétée en récupérant à partir des relations de généralisation de la pluralité de structures taxinomiques et de manière récursive, un ensemble comportant les attributs valués plus généraux et n'ayant pas déjà été présents dans la description d'une autre alerte précédemment complétée.

Selon un aspect particulier de l'invention, les attributs valués dans la structure taxinomique sont organisés selon un graphe acyclique dirigé.

L'invention vise aussi un programme informatique conçu pour mettre en œuvre le procédé ci-dessus, lorsqu'il est exécuté par le système de gestion d'alertes.

Brève description des dessins

D'autres particularités et avantages de l'invention ressortiront à la lecture de la description faite, ci-après, à titre indicatif mais non limitatif, en référence aux dessins annexés, sur lesquels :

-la figure 1 est une vue très schématique d'un système de sécurité d'informations comportant un système de gestion d'alertes selon l'invention ;

-la figure 2 est un organigramme illustrant les étapes du procédé de gestion d'un ensemble d'alertes, selon l'invention ;

-la figure 3A illustre un exemple d'une documentation associée à des signatures d'attaques ; et

-la figure 3B montre de façon très schématique une structure taxinomique associée à l'exemple de la figure 3A.

Description détaillée de modes de réalisation

La figure 1 illustre un exemple d'un système de détection d'intrusions 1 relié à travers un routeur 3 à un réseau externe 5 et à un réseau interne 7a et 7b à architecture distribuée.

Le système de détection d'intrusions 1 comporte plusieurs sondes de détection d'intrusions 11a, 11b, 11c, et un système de gestion d'alertes 13. Ainsi, une première sonde 11a de détection d'intrusions surveille les alertes venant de l'extérieur, une deuxième sonde 11b surveille une partie du réseau interne 7a comprenant des stations de travail 15 et une troisième sonde 11c surveille une autre partie du réseau interne 7b comprenant des serveurs 17 délivrant des informations au réseau externe 5.

Le système de gestion d'alertes 13 comporte un hôte 19 dédié au traitement des alertes, un système de fichiers logique 21, et une unité de sortie 23.

Le système de fichiers logique peut être du type « LISFS » proposé par Padioleau et Ridoux, dans une conférence (Usenix Annual Technical Conference 2003) intitulée "A Logic File System".

Dans le système de fichiers logique LISFS, les fichiers sont des objets auxquels sont associées des descriptions, exprimées dans une logique propositionnelle. La description d'un fichier est une conjonction de propriétés.

Les propriétés des fichiers sont les répertoires du système de fichiers, si bien que le chemin d'un fichier est sa description. Un chemin est donc une formule logique. Un emplacement du système de fichiers contient l'ensemble des fichiers dont la description satisfait la formule correspondant au chemin de l'emplacement.

Comme dans un système de fichiers classique, des commandes spécifiques permettent de naviguer et manipuler les fichiers et leurs descriptions.

Ainsi, les sondes 11a, 11b, 11c déployées dans le système de détection d'intrusions 1 envoient (flèches 26) leurs alertes 25 au système

de gestion d'alertes 13. Ce dernier, conformément à l'invention, procède à une gestion de cet ensemble d'alertes et à son stockage dans le système de fichiers logique 21 pour en permettre la consultation à travers l'unité de sortie 23 d'une manière flexible.

En effet, l'hôte 19 du système de gestion d'alertes 13 comprend des moyens de traitements pour procéder à cette gestion des alertes.

Ainsi, un programme informatique conçu pour mettre en œuvre la présente invention peut être exécuté par le système de gestion d'alertes.

La figure 2 est un organigramme illustrant les étapes du procédé de gestion d'un ensemble $\mathcal{O}$ d'alertes issues de sondes de détection d'intrusions selon l'invention.

Chaque alerte o de cet ensemble $\mathcal{O}$ d'alertes est définie par un identifiant d'alerte et un contenu d'alerte.

En effet, une alerte $o \in \mathcal{O}$ peut être définie par un identifiant d'alertes unique $id(o)$ donné par un couple (s,n) où s est l'identifiant de série de la sonde de détection d'intrusions qui produit l'alerte et n est un numéro de série d'alerte affecté par cette sonde à l'alerte o.

Le contenu m_o de l'alerte o comporte un message textuel fourni par la sonde de détection d'intrusions qui a produit l'alerte et qui est destiné à l'opérateur de sécurité.

L'étape E1 consiste à associer à chacune des alertes issues des sondes de détection d'intrusions 11a, 11b, 11c, une description $d(o)$ comportant une conjonction d'une pluralité d'attributs valués $\{d_{o,i}\}$ appartenant à une pluralité ou un ensemble de domaines d'attributs $\{\mathcal{A}\}$.

Ainsi, une description $d(o)$ d'une alerte est une conjonction de p attributs valués, c'est-à-dire $d(o) = d_{o,1} \wedge \cdots \wedge d_{o,p}$.

Un attribut valué $d_{o,i}$ est un couple (a,v) comportant un identifiant d'attribut a et une valeur d'attribut v.

Chaque identifiant d'attribut a est associé à un domaine d'attribut $\mathcal{A}$ parmi les domaines suivants : domaine de l'attaque, domaine de l'identité de l'attaquant, domaine de l'identité de la victime et domaine de la date de l'attaque.

D'une manière générale, un domaine d'attribut $\mathcal{A}$ est formé d'un ensemble discret muni d'une relation d'ordre partiel $\prec_A$ définissant le domaine de l'attribut valué $d_{o,i}$.

L'étape E2 consiste à organiser les attributs valués $d_{o,i}$ appartenant à chaque domaine d'attribut $\mathcal{A}$ en une structure taxinomique définissant des relations de généralisation (ou spécialisation) entre ces attributs valués. Il existe une taxinomie par domaine d'attribut. Ainsi, la pluralité des domaines d'attributs forme une pluralité de structures taxinomiques.

La structure taxinomique des attributs valués est de manière générique un graphe acyclique dirigé.

Les relations taxinomiques sont modélisées par des axiomes. Ainsi, un attribut valué d plus spécifique qu'un autre attribut valué d' est modélisé par un axiome $d \models d'$, c'est-à-dire que l'attribut valué d' est une conséquence logique de l'attribut valué d. Autrement dit, une alerte qui possède l'attribut valué spécifique d possède automatiquement l'attribut valué moins spécifique d'.

L'étape E3 consiste à compléter la description de chacune des alertes issues des sondes de détection d'intrusions 11a, 11b, 11c, par des ensembles de valeurs induites par les structures taxinomiques, à partir des attributs valués de ces alertes initiales, pour former des alertes complètes.

En effet, les attributs valués des alertes produites par les sondes de détection d'intrusions sont les plus spécifiques des taxinomies.

Ainsi, à la réception d'une alerte donnée, le système de gestion d'alertes 13 peut par exemple compléter la description de cette alerte en récupérant à partir des relations de généralisation de la pluralité de structures taxinomiques et de manière récursive, un ensemble comportant les attributs valués plus généraux et n'ayant pas déjà été présents dans la description d'une autre alerte précédemment complétée.

Autrement dit, la description d'une alerte donnée est complétée par un processus qui consiste à remonter dans une taxinomie donnée à partir d'un attribut valué donné. Si un attribut valué existe déjà dans la description d'une autre alerte précédemment traitée, alors le processus de remontée s'arrête, sinon il est ajouté et le processus est réitéré à partir de cet attribut valué ajouté.

Ci-dessous est un exemple d'un algorithme « *CompléterDescription* » décrivant un processus pour compléter la description d'une alerte.

CompléterDescription
s'il n'existe pas $d_{o,i}$ ***faire***
$D = \left\{ d'_{o,i} : \mathrm{d_{o,i}} \models d'_{o,i} \right\}$
pour chaque $d'_{o,i} \in D$ ***faire***
CompléterDescription($d'_{o,i}$)
fait
mkdir $d'_{o,1} / \cdots / d'_{o,n}$
fait

Cet algorithme teste tout d'abord l'existence d'un attribut valué donné $d_{o,i}$. Si cet attribut $d_{o,i}$ n'existe pas, on récupère l'ensemble $D = \left\{ d'_{o,i} : \mathrm{d_{o,i}} \models d'_{o,i} \right\}$ des attributs valués qui sont plus abstraits au regard des taxinomies. Ensuite pour chaque élément $d'_{o,i}$ appartenant à D, l'algorithme *CompléterDescription* est appelé récursivement. A la fin, l'attribut valué est ajouté au système de gestion d'alertes par la

commande « *mkdir* » qui fait partie des commandes du système de fichiers logique LISFS.

Finalement l'étape E4 de la figure 2, consiste à stocker les alertes, qui ont été complétées à l'étape précédente, dans le système de fichiers logique 21 pour en permettre la consultation.

Ci-dessous est un exemple d'un algorithme « *StockerAlerte* » décrivant un processus pour stocker une nouvelle alerte dans un système de fichiers logique du type LISFS.

StockerAlerte
Pour chaque $d_{o,i}$ ***faire***
CompléterDescription($d_{o,i}$)
fait
cp $m_o\ d_{o,1}/\cdots/d_{o,n}/a$

Cet algorithme complète de manière itérative pour chaque élément de description $d_{o,i}$, une alerte donnée o en appelant l'algorithme « *CompléterDescription* » décrit ci-dessus.

Lorsque tous les éléments de description de l'alerte donnée sont complétés, alors l'alerte complète et son contenu sont stockés par une commande de stockage « *cp* », qui prend en paramètre le contenu de l'alerte m_o, la description de l'alerte $d_{o,1}/\cdots/d_{o,n}$ et l'identifiant de l'alerte a.

Le stockage des alertes complètes dans le système de fichiers logique 21 permet leur consultation par une succession d'interrogations et/ou de navigations dans l'ensemble des alertes complètes.

Ainsi, en réponse à une requête d'un opérateur de sécurité, le système de gestion d'alertes 13 fournit des attributs valués pertinents permettant de distinguer un sous-ensemble d'alertes complètes parmi un ensemble d'alertes complètes satisfaisant la requête afin de permettre le raffinement de cette requête.

Une requête de l'opérateur de sécurité est une formule logique f, qui combine des conjugaisons $\wedge$, des disjonctions $\vee$, et des négations $\neg$ d'attributs valués.

D'une manière générale, la description $d(o)$ d'une alerte o satisfait une requête f, si la requête f est une conséquence logique de la description $d(o)$. L'ensemble des alertes satisfaisant la requête f, appelé l'extension de f, est ainsi donné par $ext(f) = \{o \in \mathcal{O} : d(o) \models f\}$.

L'ensemble A des attributs valués pertinents est l'ensemble des attributs valués appartenant à des domaines d'attributs valués $\mathcal{A}$, tel que pour tout attribut valué pertinent p de $\mathcal{A}$, l'ensemble d'alertes complètes satisfaisant la conjonction de la requête courante f avec l'attribut valué pertinent p est contenu strictement dans l'ensemble d'alertes complètes satisfaisant la requête courante f. Ainsi, cet ensemble A des attributs valués pertinents qui permettent de distinguer des alertes entre elles, peut être défini de la façon suivante :

$$A = \{p \in \mathcal{A} : \phi \subset ext(f \wedge p) \subset ext(f)\}.$$

L'ensemble $\mathcal{A}$ peut être considéré comme un ensemble des liens de navigation, en définissant chaque attribut valué pertinent p comme un lien de navigation. L'opérateur de sécurité peut ainsi raffiner sa requête courante f en choisissant un lien de navigation $p \in A$ fourni par le système de gestion d'alertes 13. La requête courante f de l'opérateur de sécurité se transforme ainsi en la nouvelle requête $f \wedge p$.

Avantageusement, pour réduire encore plus le nombre de réponses, le système de gestion d'alertes 13 fournit, en priorité, les attributs valués pertinents les plus généraux en regard de la pluralité de structures taxinomiques.

L'ensemble A_{max} des attributs valués pertinents les plus généraux est alors donné par l'ensemble $\max_{|=}(A)$ qui peut être défini de la façon suivante :

$$\max_{|=}(A) = \{ p \in A : \textit{il n'existe pas } p' \in A, p' \neq p, p \models p' \}.$$

Ainsi, cet ensemble $\max_{|=}(A)$, est l'ensemble de tout attribut valué pertinent p de A qui n'a pas un attribut valué plus général.

En outre, en réponse à la requête courante f, le système de gestion d'alertes fournit un ensemble O d'identifiants d'alertes dont la description satisfait la requête courante f et ne pouvant pas être raffinée, c'est-à-dire décrite plus précisément, par rapport à cette requête f. Ainsi, l'ensemble O des identifiants d'alertes comporte tout identifiant d'alerte dont la description satisfait la requête courante f et telle qu'il n'existe aucun attribut valué pertinent p tel que la conjonction de f et de p soit satisfaite par la description de cette même alerte. Ainsi, cet ensemble O peut être défini de la façon suivante :

$O = \{ id(o) : o \in \mathcal{O},\ d(o) \models f$, et il n'existe pas $p \in A$ avec $d(o) \models f \wedge p \}$.

On notera que le système de fichiers logique 21 tel que LISFS offre des commandes permettant de naviguer (commande « cd »), interroger (commande « ls »), et stocker (commandes « cp » et mkdir ») des objets.

Par exemple, dans LISFS, une requête permettant d'obtenir les alertes dont la victime est un *proxy web* et dont l'attaquant n'est pas interne s'exprime de la façon suivante :

ls / "victime web proxy"/! "attaquant interne".

D'une manière générale, une alerte provenant d'une sonde de détection d'intrusions est un quadruplet d'attributs valués. Les quatre attributs envisagés sont : *attaque, attaquant, victime, et date.*

Le domaine de l'attribut valué « *attaque* » est constitué des identifiants de signatures d'attaques contenus dans les alertes générées par les sondes de détection d'intrusions 11a, 11b, 11c.

Le domaine de l'attribut valué d'attaque comporte aussi les vulnérabilités éventuellement exploitées par une attaque. Les vulnérabilités sont plus abstraites, c'est-à-dire plus générales, que les identifiants d'attaques.

Les autres valeurs utilisées pour qualifier les attaques sont issues des mots clés employés pour qualifier les attaques dans une documentation des sondes de détection d'intrusions 11a, 11b, 11c.

A titre d'exemple, on peut utiliser la sonde Snortl™ et le champ « *msg* » de la documentation des signatures.

En effet, la figure 3A illustre un exemple de documentation associée aux signatures d'attaques.

La colonne 31 du tableau 33 comporte des nombres entiers désignant les signatures d'attaques. La colonne 35 du tableau 33 comporte les documentations associées à ces signatures d'attaques. Ainsi, dans chaque ligne du tableau 33, une documentation est associée à chaque signature d'attaque. Chaque description comporte des mots clés relatifs par exemple au type d'attaque, au protocole réseau utilisé, et au succès ou à l'échec de l'attaque.

La figure 3B montre une structure taxinomique 37 définissant des relations de généralisation 39 entre les attributs valués contenus dans le tableau 33. Cette structure taxinomique 37 est organisée selon des connaissances expertes, à partir des mots clés de la documentation des signatures du tableau 33. On notera que, les signatures d'attaques 31 constituent les attributs valués les plus spécifiques.

Le domaine de l'attribut valué « attaquants » comporte des adresses IP. Les adresses IP externes sont généralisables par le nom de l'organisme propriétaire de la plage d'adresses IP à laquelle appartient

l'adresse. Le nom de l'organisme correspond au champ « *netname* » contenu dans des bases de données de l'organisme IANA™, qui gère l'attribution d'adresses IP.

Les adresses IP internes et les adresses IP privées (non routables), sont généralisables en identifiants de réseaux locaux définis par un administrateur du système de détection d'intrusions 1.

Enfin les noms des organismes sont généralisables en la valeur « *ext* » et les identifiants des réseaux locaux sont généralisables en la valeur « *int* ».

Le domaine de l'attribut valué « *victime* » comporte des adresses IP. Ces adresses IP des victimes peuvent être généralisées en l'adresse du réseau local correspondant.

Ces adresses IP peuvent aussi être généralisées en noms de machines, obtenus par des mécanismes de résolution de noms. Les noms de machines peuvent être généralisés en « *fonctions* » d'hôtes (par exemple serveur web), définis par l'administrateur du site. Les noms de machines sont généralisables en identifiants de réseaux locaux définis par l'administrateur du réseau (par exemple DMZ).

Le domaine de l'attribut valué « date » comporte l'horodatage des alertes au format JJ-MM-AAAA hh:mm:ss. Les dates sont généralisées successivement en minutes, heure, jour, et mois dans l'année. Ces généralisations correspondent finalement à des abstractions de plus en plus grossières de la date d'une attaque.

Revendications

1.Procédé de gestion d'un ensemble d'alertes issues de sondes de détection d'intrusions (11a, 11b, 11c) d'un système de sécurité d'informations (1) comportant un système de gestion d'alertes (13), chaque alerte étant définie par un identifiant d'alerte et un contenu d'alerte, caractérisé en ce qu'il comporte les étapes suivantes :

-associer à chacune des alertes issues des sondes de détection d'intrusions (11a, 11b, 11c), une description comportant une conjonction d'une pluralité d'attributs valués appartenant à une pluralité de domaines d'attributs ;

-organiser les attributs valués appartenant à chaque domaine d'attributs en une structure taxinomique définissant des relations de généralisation entre lesdits attributs valués, la pluralité des domaines d'attributs formant ainsi une pluralité de structures taxinomiques ;

-compléter la description de chacune desdites alertes par des ensembles de valeurs induites par les structures taxinomiques à partir des attributs valués desdites alertes pour former des alertes complètes ;

-stocker lesdites alertes complètes dans un système de fichiers logique (21) pour en permettre la consultation.

2.Procédé selon la revendication 1, caractérisé en ce que la consultation des alertes complètes est réalisée par une succession d'interrogations et/ou de navigations dans lesdites alertes complètes de sorte qu'en réponse à une requête, le système de gestion d'alertes (13) fournit des attributs valués pertinents permettant de distinguer un sous-ensemble d'alertes complètes parmi un ensemble d'alertes complètes satisfaisant la requête afin de permettre le raffinement de ladite requête.

3.Procédé selon la revendication 2, caractérisé en ce que les attributs valués pertinents sont en priorité les plus généraux au regard de la pluralité de structures taxinomiques.

4.Procédé selon l'une quelconque des revendications 2 et 3, caractérisé en ce qu'en réponse à la requête, le système de gestion d'alertes (13) fournit en outre des identifiants d'alertes satisfaisant la requête et dont la description ne peut pas être raffinée par rapport à ladite requête.

5.Procédé selon la revendication 1, caractérisé en ce que l'identifiant d'alerte est un couple formé d'un identifiant de la sonde de détection d'intrusions (11a, 11b, 11c) qui produit l'alerte et d'un numéro de série d'alerte affecté par ladite sonde.

6.Procédé selon la revendication 1, caractérisé en ce que le contenu de chaque alerte comporte un message textuel fourni par la sonde de détection d'intrusions (11a, 11b, 11c) correspondante.

7.Procédé selon l'une quelconque des revendications 1 à 6, caractérisé en ce que chaque attribut valué comporte un identifiant d'attribut et une valeur d'attribut.

8.Procédé selon la revendication 7, caractérisé en ce que chaque identifiant d'attribut est associé à un domaine d'attributs parmi les domaines suivants : domaine de l'attaque, domaine de l'identité de l'attaquant, domaine de l'identité de la victime et domaine de la date de l'attaque.

9.Procédé selon la revendication 1, caractérisé en ce que la description d'une alerte donnée est complétée en récupérant à partir des relations de

généralisation de la pluralité de structures taxinomiques et de manière récursive, un ensemble comportant les attributs valués plus généraux et n'ayant pas déjà été présents dans la description d'une autre alerte précédemment complétée.

10.Procédé selon l'une quelconque des revendications 1 à 9, caractérisé en ce que les attributs valués dans la structure taxinomique sont organisés selon un graphe acyclique dirigé.

11. Programme informatique caractérisé en ce qu'il est conçu pour mettre en œuvre le procédé selon l'une quelconque des revendications 1 à 10 lorsqu'il est exécuté par le système de gestion d'alertes (13).

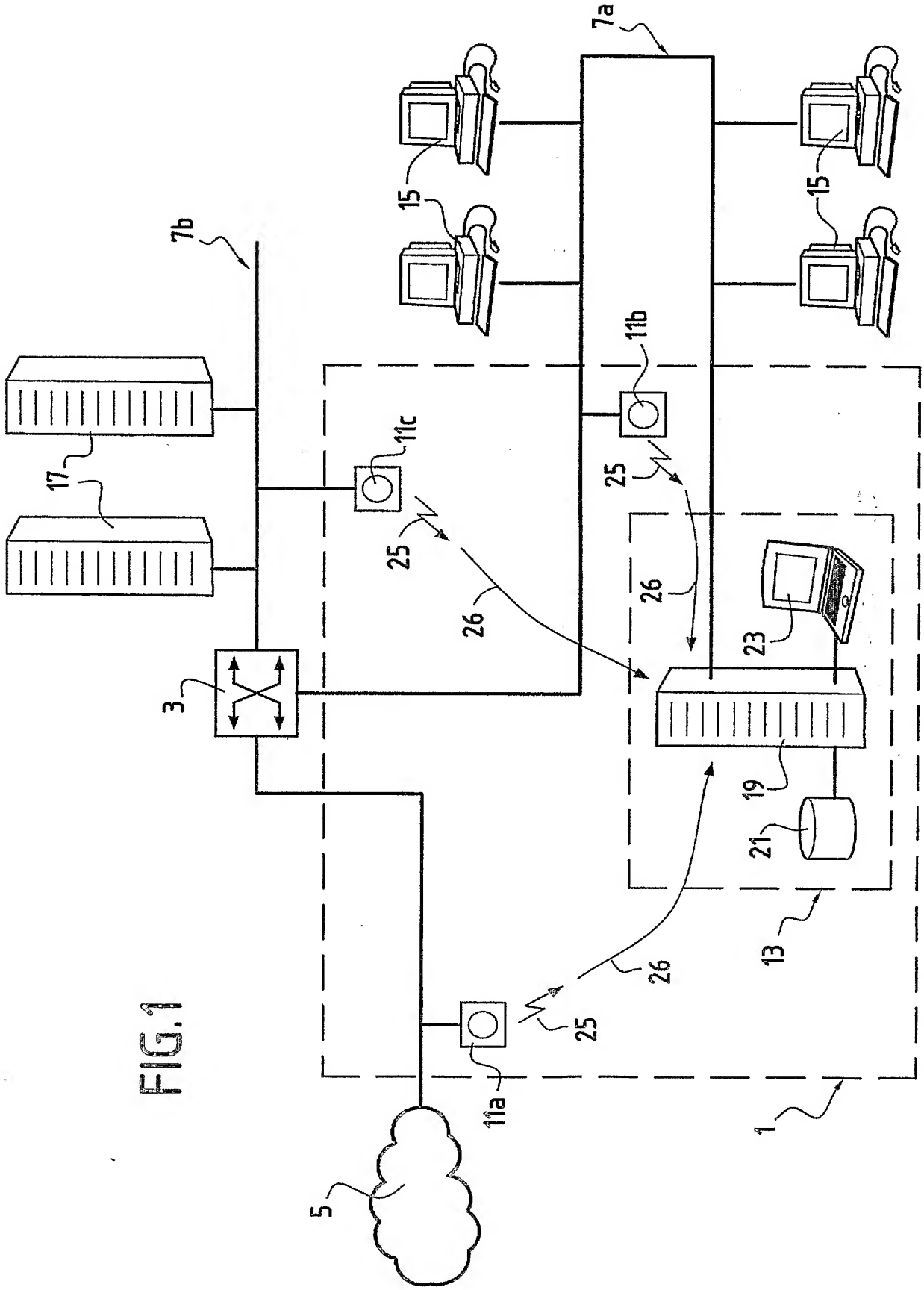

FIG.1

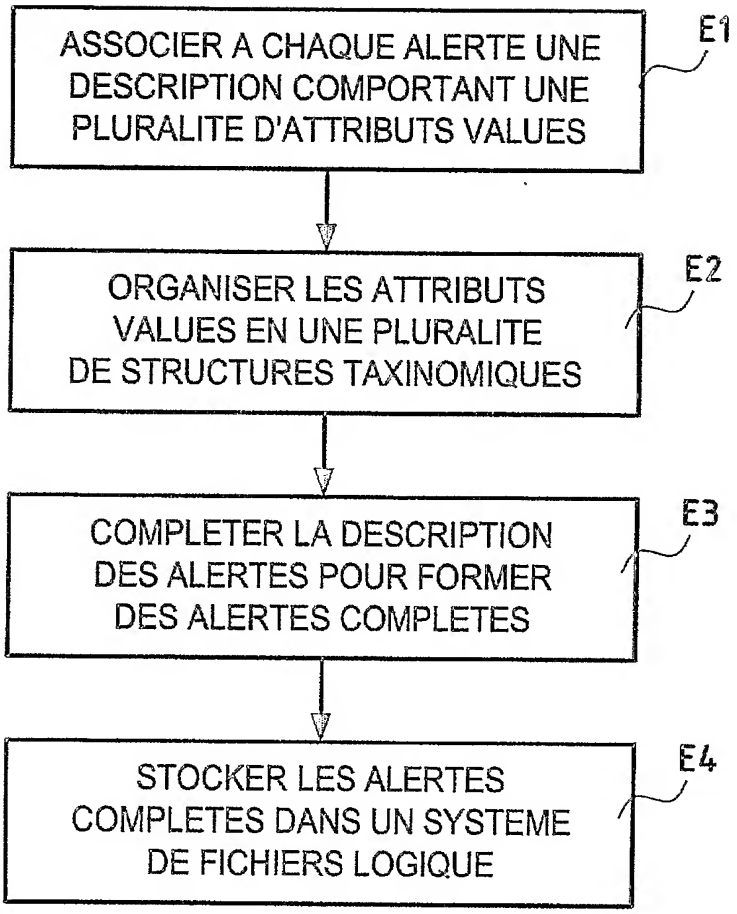
ASSOCIER A CHAQUE ALERTE UNE DESCRIPTION COMPORTANT UNE PLURALITE D'ATTRIBUTS VALUES
E1
ORGANISER LES ATTRIBUTS VALUES EN UNE PLURALITE DE STRUCTURES TAXINOMIQUES
E2
COMPLETER LA DESCRIPTION DES ALERTES POUR FORMER DES ALERTES COMPLETES
E3
STOCKER LES ALERTES COMPLETES DANS UN SYSTEME DE FICHIERS LOGIQUE
E4

FIG.2

31 35

Sig. Id	Documentation
1739	WEB-PHP DNSTools administror authentication bypass attempt (tentative de contournement de l'authentification de l'administrateur)
1740	WEB-PHP DNSTools authentication bypass attempt (tentative de contournement de l'authentification)
1741	WEB-PHP DNSTools access (accès)
803	WEB-CGI HyperSeek hsx.cgi directory traversal attempt (tentative de remontée de répertoire)
1076	WEB-IIS repost.asp access (accès)
1110	WEB-MISC apache source.asp file access (accès au fichier)
340	FTP EXPLOIT overflow (débordement de zone mémoire)
1247	WEB-FRONTPAGE rad overflow attempt (tentative de débordement de zone mémoire)

33

FIG.3A

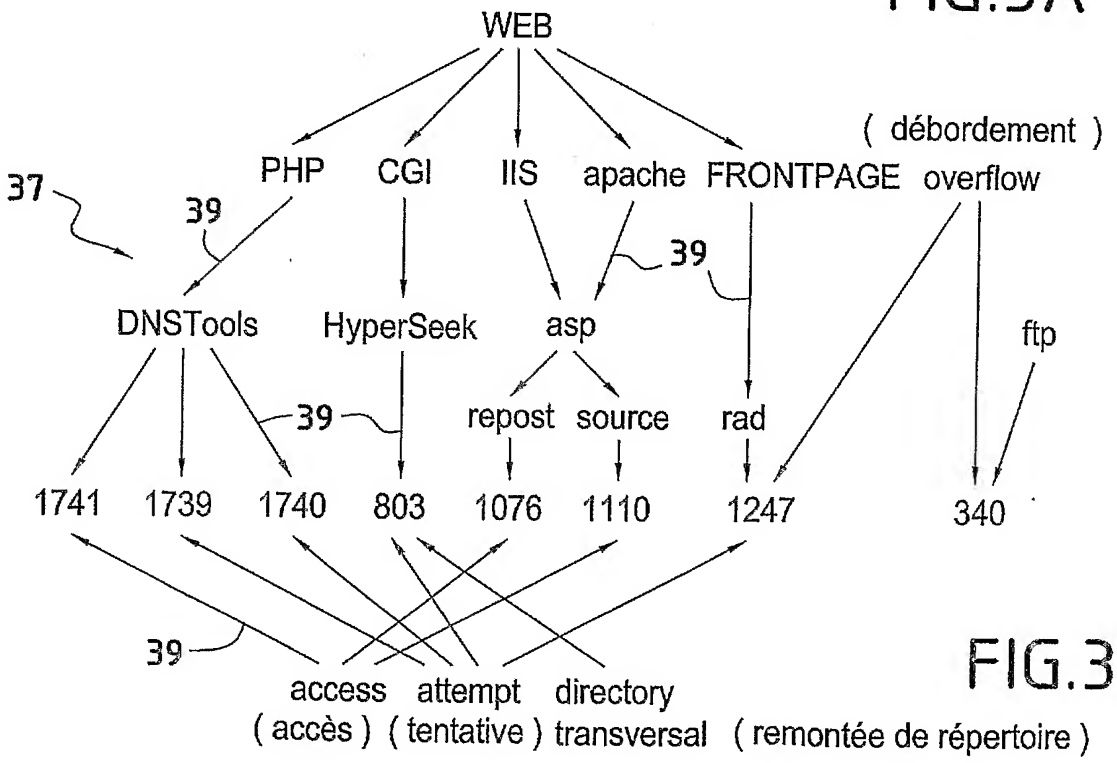

FIG.3B

reçue le 17/05/04

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

certifié
N° 11235*03

DÉPARTEMENT DES BREVETS
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

DÉSIGNATION D'INVENTEUR(S) Page N° 1/1

(À fournir dans le cas où les demandeurs et les inventeurs ne sont pas les mêmes personnes)

INV

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 W / 270601

Vos références pour ce dossier *(facultatif)*	1H518040/22.SY
N° D'ENREGISTREMENT NATIONAL	0314833

TITRE DE L'INVENTION (200 caractères ou espaces maximum)

Procédé de gestion d'un ensemble d'alertes issues de sondes de détection d'intrusions d'un système de sécurité d'informations.

LE(S) DEMANDEUR(S) :

FRANCE TELECOM

DESIGNE(NT) EN TANT QU'INVENTEUR(S) :

1 Nom		MORIN
Prénoms		Benjamin
Adresse	Rue	22, rue des Croisiers
	Code postal et ville	14000 CAEN
Société d'appartenance *(facultatif)*		
2 Nom		DEBAR
Prénoms		Hervé
Adresse	Rue	7, rue des Semailles
	Code postal et ville	14111 LOUVIGNY
Société d'appartenance *(facultatif)*		
3 Nom		
Prénoms		
Adresse	Rue	
	Code postal et ville	
Société d'appartenance *(facultatif)*		

S'il y a plus de trois inventeurs, utilisez plusieurs formulaires. Indiquez en haut à droite le N° de la page suivi du nombre de pages.

DATE ET SIGNATURE(S)
DU (DES) DEMANDEUR(S)
OU DU MANDATAIRE
(Nom et qualité du signataire)

CABINET BEAU DE LOMENIE
Jean-Jacques JOLY
CPI N° 92-1123
Paris, le 17 décembre 2003